IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Jamal Benbrahim	Attorney Docket No.: IGT1P376/P-227
Application No.: 09/880,474	Examiner: Emmanuel Omotosho
Filed: June 12, 2001	Group: 3714
Title: METHOD AND APPARATUS FOR SECURING GAMING MACHINE OPERATING DATA	Confirmation No.: 5212

CERTIFICATE OF EFS-WEB TRANSMISSION
I hereby certify that this correspondence is being transmitted electronically through EFS-WEB to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450 on November 29, 2007.

Signed: /swx/
Susan W. Xu

APPLICANT INITIATED INTERVIEW REQUEST FORM

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Tentative Participants:

1) Ray Mahboubian
2) Examiner Emmanuel Omotosho
3)
4)

Proposed Date of Interview: **TO BE DECIDED** Proposed Time: **2:00 PM (Eastern Time)**

Type of Interview Requested:

☒ Telephone ☐ Personal ☐ Video Conference

Exhibit to be Shown or Demonstrated: ☐ Yes ☐ No
If yes, provide brief description:

ISSUES TO BE DISCUSSED

Issues (Rej., Obj., etc.)	Claims/ Fig., #s	Prior Art	Discussed	Agreed	Not Agreed
1) 103	Claim 18	*Graunke et al*	☐	☐	☐
2)			☐	☐	☐
3)			☐	☐	☐

BRIEF DESCRIPTION OF AGRUMENTS TO BE PRESENTED:

Claim 18 has been amended to further clarify the subject matter regarded as the invention. New claims 37-40 pertain to operations that can be performed by a remote device in connection with a gaming device (see, for example, claim 18).

In the Office Action, the Examiner has rejected claims 18-36 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,645,077 (*Rowe*) in view of U.S. Patent No. 5,991,399 (*Graunke et al.*) and Patent No. 6,149,522 (*Alcorn et al.*). The Examiner's rejection of claims is fully traversed below.

Claim 18, among other things, recites:

> *a) receiving by a gaming device only one of a first private key or a second private key for respectively decrypting encrypted first and second operating data which are stored on a gaming device for first and second games, in order to prevent the executing of the first or second game on the gaming device, and*
>
> *b) sending by the gaming device information related to the decrypted one of the first or second operating for authentication after decrypting it respectively by the first or second private key.*

Initially, it is respectfully submitted that the Examiner has not properly addressed these claimed features (a and b noted above). Instead, the Examiner has merely asserted that *Graunke et al.* teaches "utilizing private key for cryptographic processing data" (Office Action, page 3). Clearly, this general assertion does not address the claimed feature of: (a) receiving by a gaming device (or providing the gaming device with) only one of a first private key or a second private key for respectively decrypting encrypted first and second operating data which are stored on a gaming device for first and second games, in order to prevent the executing of the first or second game on the gaming device.

Accordingly, it is respectfully submitted that the Examiner's rejection is improper and should be withdrawn. Moreover, it is respectfully submitted that *Graunke et al.* does not teach this claimed feature (a). Instead, *Graunke et al.* teaches: secure distribution of a private key to a user's application program (such as DVD player) with

conditional access based on verification of the application program (see, for example, the Abstract).

In the Office Action, the Examiner has asserted that *Alcorn et al.* teaches the claimed feature of: (b) sending by the gaming device information related to the decrypted one of the first or second operating for authentication after decrypting it respectively by the first or second private key. In order to support this assertion, the Examiner has relied on the abstract of *Alcorn et al.* which is reproduced below:

> Authentication of a casino game data set is carried out within the casino game console using an authentication program stored in an unalterable ROM physically located within the casino game console. The casino game data set and a unique signature are stored in a mass storage device, which may comprise a read only unit or a read/write unit and which may be physically located either within the casino game console or remotely located and linked to the casino game console over a suitable network. The authentication program stored in the unalterable ROM performs an authentication check on the casino game data set at appropriate times, such as prior to commencement of game play, at periodic intervals or upon demand. At appropriate occasions, the contents of the unalterable ROM can be verified by computing the message digest of the unalterable ROM contents and comparing this computed message digest with a securely stored copy of the message digest computed from the ROM contents prior to installation in the casino game console.
> [*Alcorn et al.* Abstract]

Clearly, the abstract of *Alcorn et al.* or general knowledge that authentication can be performed does not address this specific claimed feature. Accordingly, it is respectfully submitted that the Examiner's rejection is improper and should be withdrawn for this additional reason.

Moreover, it is respectfully submitted that the cited art does not teach or suggest the combination of the claimed features noted above (a and b) and therefore claim 18 and other independent claims are patentable over the cited art for at least this reason.

Finally, it is respectfully submitted that the Examiner has failed to establish a prima facie case of obviousness because the Examiner has failed to provide a motivation or suggestion for combining *Rowe*, *Graunke et al.* and *Alcorn et al*. Instead, the Examiner has merely asserted that "one of ordinary skill in the art would have been forced to seek outside references, such as the *Graunke et al.* reference for disclosure

as to the known manners and/or procedures of enacting the encryption as described in the first invention of Rowe" (Office Action, page 4), and *Alcorn et al.* teaches "a step of taking the security measures a step further to prevent tampering with the contents of the game data" (Office Action, page 5).

An interview was conducted on the above-identified application on .

*Note: This form should be completed be applicant and submitted to the examiner in advance of the interview (see MPEP §713.01). This application will not be delay from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFT 1.33(b)) as soon as possible.

(Applicant/Applicant's Representative) Signature)	(Examiner/SPE Signature)

18. (Currently Amended) A method of operating a gaming device, the method comprising:

receiving from a remote device encrypted executable code for a plurality of games including a first game and a second game, wherein the first game includes a first set of operating data for at least one of first audio data or first video data for generating the first game on the gaming device, and the first set of operating data is encrypted with a first private key, and wherein the second game includes a second set of operating data for at least one of second audio data or second video data for generating the second game on the gaming device, and the second set of operating data is encrypted with a second private key;

~~providing~~ storing on the gaming device the encrypted executable code for [[a]] the plurality of games including ~~a first game~~ the first set of operating data for the first game and ~~a second game~~ the second set of operating data for the second game~~, each of the plurality of games stored in an encrypted format, wherein the plurality of games comprise at least a first set of operating data for the first game comprising at least one of first audio data or first video data for generating the first game on the gaming device, and wherein the first set of operating data is encrypted with a first private key and storing a second set of operating data for the second game comprising at least one of second audio or second video data for generating the second game on the gaming device, wherein the second set of operating data is encrypted with a second private key~~;

~~providing~~ receiving by the gaming device from the remote device ~~with~~ only one of the first private key or the second private key in order to prevent execution of the first game or the second game on the gaming device;

decrypting, by the gaming device, one of the first set of operating data or the second set of operating data according to the one of the first private key or the second private key selected to recover the one of the first set of operating data or the second set of operating data;

sending, by the gaming device, information relating to the decrypted one of the first set of operating data or the second set of operating data to a remote device for authentication of the decrypted one of the first set of operating data or the second set of operating data after decrypting one of the first set operating data or the second set of operating data;

taking remedial action by the gaming device when the decrypted one of first set of operating data or the second set of operating data is not authenticated by the remote device, wherein the remedial action includes not allowing the decrypted one of first set of operating data or the second set of operating data to be executed by the gaming device;

storing the decrypted one of the first set of operating data or the second set of operating data on the gaming device when the decrypted one is authenticated by the remote device; and

executing the first game or the second game on the gaming device utilizing the decrypted one of the first set of operating data or the second set of operating data when the decrypted one is authenticated by the remote device.